APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,483	11/17/2003	Simon Charles Watt	550-471	6434

23117   7590   08/21/2007
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER
JOHNSON, BRIAN P

ART UNIT	PAPER NUMBER
2183	

MAIL DATE	DELIVERY MODE
08/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/714,483
Filing Date: November 17, 2003
Appellant(s): WATT ET AL.

MAILED

AUG 2 1 2007

Technology Center 2100

Stanley C. Spooner
Reg. No. 27,393
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 26 April 2007 appealing from the Office action mailed 02 November 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendments after final were made.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claim Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Alverson (U.S. Patent No. 7,020,767)

Angelo (U.S. Patent No. 6,581,162)

Christensen (U.S. Patent No. 5,752013)

Faccin (U.S. Patent No. 6,879,690)

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-8, 10-16, 18-36 and 38-39 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Alverson's background (U.S. Patent No. 7,020,767) in view of

Angelo (U.S. Patent No. 6,581,162).

Regarding claim 1, Averson discloses a system with multiple domains.

Alverson also discloses a protection requirement for the domains, but fails to

disclose particular information about monitoring.

Angelo discloses a monitoring function within a processing system (col 7 line 40

to col 8 line 15).

Alverson, at the time of the invention, would have been motivated to use SMM

and SMI in computer security memory management to protect against malicious

software and viruses, thereby improving computer security memory management.

Furthermore, Alverson has shown an expressed desire for multiple levels of protection

that is domain specific (col 2 line 56-57).

It would have been obvious at the time of the invention for one of ordinary skill in

the art to take the system of Alverson and incorporate the SMM and SMI security of

Angelo. The combination would be as follows:

Alverson/Angelo method of controlling a monitoring function of a processor

(Angelo col 7 line 40 to col 8 lines 15), said processor being operable in at least two

domains (col 1 lines 30-33), comprising a first domain and a second domain, said first

and second domains each comprising at least one mode (Angelo col 7 line 61 to col 8

line 4), said method comprising the steps of: controllably monitoring (Angelo col 7 line

56-58) said processor operating in each of said at least two domains (col 1 lines 30-33

and col 2 lines 56-57—*Note that the citations indicate that Alverson desired a level of

security that can vary in each domain*), setting at least one control value, said at least

one control value (col 7 lines 56-58) relating to a condition and being indicative of

whether said monitoring function is allowable in said first domain (Angelo col 7 line 61 to

col 8 line 4); and only allowing initiation of said monitoring function in said first domain

when said condition is present if its related control value indicates that said monitoring

function is allowable; and not allowing initiation of said monitoring function in said first

domain when said condition is present and its related control value indicates that said

monitoring function is not allowable (Angelo col 7 line 61 to col 8 line 4).

Regarding claim 2, Alverson/Angelo discloses the method according to claim 1,

wherein said first domain is a secure domain and said second domain is a non-secure

domain (Angelo col 8 line 4), said processor being operable such that when executing a

program in a secure mode within said secure domain said program has access to

secure data which is not accessible when said processor is operating in a non-secure

mode within said non-secure domain (Angelo col 8 line 11-15).

Note that a domain is considered to be in a secure mode when the SMI handler is running. At this point, it is a "secure domain". Otherwise, it is non-secure.

Regarding claim 3, Alverson/Angelo discloses the method according to claim 2, wherein said condition comprises a domain, mode or type of monitoring function (Angelo col 7 line 61 to col 8 line 4).

Regarding claim 4, Alverson/Angelo discloses the method according to claim 3, wherein said condition comprises a secure domain and said control value comprises a secure domain enable value, initiation of monitoring in said secure domain only being allowed if said secure domain enable value is set (Angelo col 7 line 61 to col 8 line 4).

Regarding claim 5, Alverson/Angelo discloses the method according to claim 3, wherein said secure domain includes a secure user mode and said condition comprises a secure user mode (Angelo col 8 line 1).

Note that the handler routine is considered to be the "secure user mode"

Regarding claim 6, Alverson/Angelo discloses the method according to claim 5 wherein said control value comprises a secure user mode enable bit (col 7 line 56-57) and initiation of monitoring from secure user mode is only allowed if said secure user mode enable bit has been set (Angelo col 7 line 61 to col 8 line 4).

Regarding claim 7, Alverson/Angelo discloses the method according to claim 4, wherein said condition comprises a type of monitoring function (Angelo col 8 line 1-4).

Regarding claim 8, Alverson/Angelo discloses the method according to claim 7, wherein said condition comprises a debug monitoring function and said control value comprises a debug enable bit, initiation of debug in said first domain only being allowable if said debug enable bit has been set (Angelo col 8 line 8-11).

Note that the monitoring function is considered to be a debug monitoring function.

Regarding claim 11, Alverson/Angelo discloses the method according to claim 1, said method comprising setting a plurality of control values, each of said plurality of control values relating to a different condition; and only allowing initiation of said monitoring function in said first domain if any of said conditions are present if each of said control values related to a condition that is present indicate that said monitoring function is allowable (Angelo col 7 line 61 to col 8 line 11).

Note that the plurality of control values includes the SMI interrupt and the SMIACT signal.

Regarding claim 12, Alverson/Angelo discloses the method according to claim 1, said method further comprising said steps of: setting a control indicator, said control indicator indicating that monitoring is only allowable for specified applications; and prior

to initialising said monitoring function checking an application identifier; and only allowing initiation of said monitoring function if said application currently running is one for which monitoring is allowable.

Note that Alverson/Angelo, as previously combined, does not necessarily disclose the limitations above. As originally combined, the SMI handler routine is domain specific; however, it would further be obvious to make these routines stream (or application) specific.

Alverson would have been motivated to utilize this technique since the invention is initially concerned with stream specific privileges (Alverson col 2 lines 56-57).

Regarding claim 13, Alverson/Angelo discloses the method according to claim 12, wherein the step of setting a control indicator comprises setting a control indicator stored in a predetermined position in a storage element.

Note that the use of a particular interrupt or signal suggests that it is held in a common register that is considered to be "a predetermined position in a storage element". More generally, in order for the signal to have the necessary effects, its position must be predetermined; otherwise, the processor would not know what the signal is attempting to signify.

Regarding claim 14, Alverson/Angelo discloses the method according to claim 12, wherein said monitoring function comprises monitoring said processor and capturing diagnostic data (Angelo col 7 line 64 to col 8 line 4), said method comprising the further

step of: following initiation of said monitoring function only allowing capturing of

diagnostic data in said first domain while an application running on said processor is

one for which monitoring is allowable (see claim 12).

Regarding claim 15, Alverson/Angelo discloses the method according to claim 1,

wherein said monitoring function comprises monitoring said processor and capturing

diagnostic data (Angelo col 7 line 64 to col 8 line 4), said method comprising the further

step of: following initiation of said monitoring function only allowing capturing of

diagnostic data in said first domain when a condition changes if a control value related

to the changed condition indicates that said monitoring function is allowable (Angelo col

8 line 8-11).

Regarding claim 16, Alverson/Angelo discloses the method according to claim 1,

wherein setting of at least one control value is performed either by setting said control

value via an input port or by setting said control value from the first domain (Angelo col

7 line 56-58).

Regarding claim 17, Alverson/Angelo discloses the method according to claim 16, said

method comprising the further step of blocking write access to said control value via

said input port such that the step of setting said control value can henceforth only be

performed by setting said control value from said first domain.

Note that the SMM signal, in some embodiments (Angelo see col 7 lines 56-58) does

not require an input port. Consequently, these embodiments are considered to be

blocked, leaving only modification from the first domain.

Regarding claim 18, Alverson/Angelo discloses the method according to claim 1,

wherein said first domain comprises a first user mode (Alverson col 1 lines 30 to 33)

and a first privileged mode (Alverson col 2 lines 56-57) and the step of setting at least

one control value in said first domain (Angelo col 8 lines 8-11), comprises setting said

control value from said first privileged mode.

Note that a level of privilege will often be activated (Alverson) when the SMI

handler routine is called (Angelo)

Regarding claims 20-28, see claims 1-9.

Regarding claim 29, Alverson/Angelo discloses the processor according to claim

20, wherein: said storage element is operable to contain a plurality of control values,

each of said plurality of control values relating to a different condition (Angelo col 7 lines

57-58 and col 8 lines 9-11); and said control logic is operable to only allow initiation of

said monitoring logic in said first domain if any of said conditions are present if each of

the control values related to a condition that is present indicate that the monitoring logic

is allowable (Angelo col 7 lines 61-64).

Regarding claim 30, Alverson/Angelo discloses the processor according to claim 29

wherein one condition comprises a secure domain and a corresponding control value

comprises a secure domain enable bit (Angelo col 7 line 61 to col 8 line 4) and a further

condition comprises a secure user mode and a corresponding control value comprises a

secure user mode enable bit (Alverson col 1 lines 30-33—*note that the secure user*

mode and secure mode of the domain are considered to be the same), said control logic

being operable to initiate said monitoring logic from secure user mode only when said

storage element contains both a secure user mode enable bit and a secure domain

enable bit (Angelo col 7 line 61 to col 8 line 4).

Regarding claim 31, Alverson/Angelo discloses the processor according to claim

20, wherein: said storage element is further operable to contain a control indicator, said

control indicator indicating that monitoring is only allowable for identified applications

(see combination used in claim 12); and said control logic is operable to check at least

one identifier identifying an application that is allowable (Angelo col 7 line 61-64), said

control logic only initiating said monitoring logic in the first domain when said application

currently running is one identified as being one for which monitoring is allowable

(Angelo col 7 line 61 to col 8 line 4).

Regarding claim 32, Alverson/Angelo discloses the processor according to claim

31, said processor comprising a further storage element, said storage element being

operable to contain said at least one identifier specifying an application that is allowable

(Alverson col 1 lines 37-38).

Regarding claim 33, Alverson/Angelo discloses the processor according to claim 31, wherein said monitoring logic is operable to monitor the processor and capture diagnostic data (Angelo col 7 liens 61-64); and wherein said control logic is operable to control the monitoring logic to suppress capturing of diagnostic data in said first domain when said control logic detects that said application running is not one identified as being allowable (Alverson col 1 lines 37-38).

Note that if the processing system hasn't picked a particular application stream to run,

then the monitoring of that application is considered to be suppressed.

Regarding claim 34, Alverson/Angelo discloses the processor according to claim 20, said processor further comprising an input port, wherein said control value is operable to be set in said storage element either via the input port or via an input from said first domain (Angelo col 7 line 56-58).

Regarding claims 34-36, see claims 16-18, respectively.

Regarding claims 38 and 39, Alverson/Angelo disclose the use of a register holding the storage elements.

Note that according to the American Heritage College dictionary, a computer science definition of a register is "a part of a central processing unit used as a storage location."

Claims 9, 10, 17 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alverson/Angelo in view of common art.

Regarding claim 9, Alverson/Angelo discloses the method according to claim 8, Alverson/Angelo discloses saving a portion of memory (Angelo col 7 lines 61-64).

Angelo fails to particularly disclose that the information includes instruction traces.

Examiner asserts that saving instruction traces is common in the art and can be utilized for many debugging purposes. Alverson/Angelo would have been motivated to utilize this technique to gather more debugging/security information for analysis. It would be further obvious to include a trace enable bit so the processor knows when to save instruction traces.

Regarding claim 10, Alverson/Angelo discloses the method according to claim 9, wherein said secure domain enable value comprises a secure debug enable bit and a secure trace enable bit, initiation of debug and trace in said secure domain only being allowable if respective portions of said secure domain enable value are set (see claim 9).

Regarding claims 17 and 37, Alverson/Angelo discloses a method according to

claim 16, wherein said first domain comprises a first user mode (Angelo col 1 lines 30-

33) and a first privileged (Alverson col 2 lines 56-57) mode and said step of setting at

least one control value in the first domain (Angelo col 8 lines 8-11),

Examiner asserts that it would have been obvious to require a non-privileged

mode, domain, etc. to require an authentication code before accessing the control value

of a privileged domain.

Examiner further asserts that Angelo/Alverson desired to have a form of security

(Alverson col 2 lines 56-57 and Angelo col 8 line 4) and would be motivated to utilize

this technique. Additionally, Angelo col 7 lines 15-24 shows the use of an authorization

code, generally.

(10) Response to Arguments

Appellant's arguments provided in the Appeal Brief are unpersuasive.

A. "Setting" of Claim 1 and "Storage Element" of Claim 20.

Appellant states:

"Appellants' independent method of claim 1 recites the step of 'setting at least
one control value, said at least one control value relating to a condition . . .' Similarly,
claim 20 recites a storage element for accomplishing the same step. . . The Examiner
alleges that this is generally disclosed somewhere in the Angelo reference. . . On page
3 of the Action, the Examiner suggests that the claimed 'setting' step in claim 1 and
'storage element' in claim 20 are taught in Angelo at column 7, lines 56-58 and that
column 7, line 61 to col 8, line 4 teaches that the control value is related to a condition
(also required by claims 1 and 20). From a detailed review of columns 7 and 8, it
appears Examiner is contending that the System Management Interrupt (SMI) is the
claimed 'control value.' A review of Angelo at columns 7 and 8 indicate that the SMIs

which are asserted is a 'non-maskable interrupt' having nothing to do with anything' relating to a condition' as in the current claims. There is no reference to a 'condition' or suggesting that anything in Angelo is dependent upon the recognition of a 'condition.' Additionally, there seems to be no stated indication by Examiner as to how or why he believes the SMI is related to or discloses the claimed 'condition.' Furthermore, there is no discussion in Angelo that discloses or even suggests that the SMI is 'indicative of whether said monitoring function is allowable in said first domain.'"

Appellant has correctly stated Examiner's position that the System Management Interrupt (SMI) is the claimed "control value." Appellant goes further to claim that the SMI is not "related to a condition" or "indicative of whether said monitoring function is allowable in said first domain." Examiner disagrees with this assertion.

Dictionary.com defines a condition as "a particular mode of being of a person or thing; existing state; situation with respect to circumstances." This is a rather broad definition. Appellant argues that the SMI is in no way related to a condition; this contention is without merit. The follow are several conditions to which the SMI is related:

1) An SMI timer can be used to assert the SMI (col 7 lines 56-57). Completion of this timer is a condition.

2) A system request can be used to assert the SMI (col 7 lines 56-67). The assertion of this system request is a condition.

3) The assertion of the SMI is used to toggle the system management mode (SMM) (col 7 lines 43-47). This mode is a condition.

Appellant further contends that the SMI is not "indicative of whether said monitoring function is allowable in said first domain." This argument is equally unpersuasive. Column 7 of Angelo under "The System Management Mode" clearly

describes how the SMI is used to enter the System Management Mode (col 7 lines 43-47). Angelo further discloses that the SMM allows the microprocessor to map a portion of memory from the SMM memory into the main memory space (in other words, monitoring) (col 7 lines 59-64). Why Appellant does not believe that the SMI is indicative of whether monitoring is allowable is unclear. This feature is disclosed quite clearly in the prior art.

The final portion of the second limitation ("in said first domain") is disclosed in Alverson (col 1 lines 30-33). The citation of Alverson indicates that the computer system has multiple domains. Each of these domains requires varying degrees of protection (col 2 lines 56-67). Therefore, as combined, Alverson/Angelo contains multiple domains (Alverson col 1 lines 30-33) with varying degrees of protection (Alverson col 2 lines 56-57) by utilizing a SMM asserted by an SMI (Angelo col 7 line 44 to col 8 lines 4).

Appellant's claim 20 requires the limitation of a "storage element operable to be set to contain at least one control value." Appellant argues that this storage element does not exist in the prior art. Examiner disagrees.

This storage element is an inherent aspect of the invention. It is clear in Angelo that a signal exists called an SMI. This SMI is set as a result of various conditions and read to result in other conditions (col 7 lines 43-47 and 56-67). Clearly, for this signal to exist it must be stored somewhere. Examiner interprets this inherent storage location to be Appellant's claimed "storage element." To argue, as Appellant apparently does, that

a control value can exist and be read but have no storage location is completely

unpersuasive.

B. More Discussion of the "Control Value"

Appellant states:

"Here, because the Examiner admits the 'control value' is not disclosed in Alverson and because he provides no identification of where this is taught in Angelo, it is clear that the Examiner has failed to meet his burden of proof."

Examiner disagrees. Appellant contends that Examiner has now shown where in

Angelo the control value is taught. It is unclear why Appellant takes this position. In the

Office Action mailed 02 November 2006, Examiner cited Angelo column 7 lines 56-68

with respect to the control value; this citation clearly discusses the SMI signal.

Furthermore, Appellant has correctly identified Examiner's interpretation of the claimed

"control value" on page 7 of this Appeal Brief: "it appears the Examiner is contending

that the System Management Interrupt (SMI) is the claimed 'control value'."

The rejection of the claim is clear, valid, and fully understood by Appellant.

Section B of this Appeal Brief appears to be a rewording of the argument in Section A.

Consequently, Examiner takes the same position as presented in Section A with respect

to the claimed "control value."

C. "Not Allowing" in Claim 1 and "Control Logic" of Claim 20.

Appellant states:

"a review of the cited portion of Angelo contains no language or suggestion even vaguely related to 'not allowing initiation of said monitoring function. . . ' Why or how the Examiner believes the 'not

allowing' or 'control logic' of the claims is hidden somewhere in Angelo is not apparent from the Office Action."

Appellant's representation of Examiner's position is incorrect. Examiner does not

believe that the claimed limitations discussed are hidden in Angelo. Rather, they are

clearly and explicitly disclosed. As discussed above, Angelo discusses the use of a

System Management Mode which is entered upon after the assertion of a System

Management Interrupt (col 7 lines 43-47). When this mode is activated, the monitoring

function begins (col 7 line 61 to col 8 line 9). This monitoring is not allowed otherwise.

If Appellant desires more evidence of this functionality, Examiner directs attention to

Angelo column 8 lines 44-50: "Because <u>SMM memory 200 is only addressable while the</u>

<u>computer system is in SM</u>, storing machine identification information 212, encryption

keys 214 and the encryption algorithm 216 in SMM memory 200 prevents malicious

code from modifying or reading these sensitive components of the disclosed

embodiment of the invention."

D. Angelo's Alleged Teaching Away from Appellants' Independent Claims

Appellant states:

> *"Appellants' independent claims specify the above-noted step of 'not allowing' the monitoring function when the 'condition' is present and the related 'control value' indicates that the monitoring function is not allowable. Contrarily, Angelo teaches that its monitoring function (i.e., entry into the System Management Mode (SMM)) is always allowed in response to an SMI (the Examiner appears to contend that the SMI is analogous to the claimed 'control value'). Because Angelo teaches that the monitoring function is always allowed, it would necessarily lead those of ordinary skill in the art away from Appellants' conditional non-allowance and thereby lead away from the combination of elements asserted by the Examiner."*

Examiner agrees that the monitoring is always allowed when the SMI is asserted

and the processor enters into SMM. This does not change the validity of the rejection.

Claim 1 requires "not allowing initiation of said monitoring function in said first domain when said condition is present and its related control value indicates that said monitoring function is not allowable." With respect to Angelo, initiation of the monitoring function is not allowed (here, SMM memory is not addressable—see col 8 lines 44-50) when the related control value indicates that the monitoring function is not allowable (here, when SMI is not activated and the computer is not in the SMM monitoring is not allowed—see col 7 lines 43-47 and 61-64).

E. Appellant Requests a Reference for Examiner's Official Notice.

Regarding claims 9 and 10, Examiner provides the prior art Christensen (U.S. Patent No. 5,752013). In particular, column 4 lines 9-23 and column 6 lines 63-67 disclose the elements that Alverson/Angelo lack.

Regarding claims 17 and 37, Examiner provides the prior art Faccin (U.S. Patent No. 6,879,690). In particular, column 1 lines 5-8 and column 2 lines 15-30 disclose the elements that Alverson/Angelo lack.

F. Rejection of Claims 1-8, 11-16, 18-36, 38 and 39

Appellant summarizes several of the Arguments with respect to Sections A-E. Examiner's position remains the same as discussed above with respect to these arguments.

Appellant further states that "at no point in the rejections does the Examiner

provide the required 'reason' or 'motivation' for combining the Alverson and Angelo

reference.".

Firstly, Appellant is reminded that motivation is not required for a rejection under

35 USC 103. See KSR International Co. v. Teleflex Inc., 550 U.S.—, 82 USPQ2d 1385

(2007).

Secondly, page 2 of The Final Office Action mailed on 02 November 2006 states,

"Alverson, at the time of the invention, would have been motivated to use SMM and SMI

in computer security memory management to protect against malicious software and

viruses, thereby improving security memory management. Furthermore, Alverson has

shown an expressed desire for multiple levels of protection that is domain specific (col 2

lines 56-67)."

Appellant has either overlooked or chosen not to address this motivation. For

that reason, it is presumed to be adequate.

G. Appellant alleges Error with the Official Notice rejection

Appellant claims that there is not motivation presented for the Official Notice

rejection of claims 9, 10, 17 and 37.

Regarding claims 9 and 10, Page 11 of the Final Office Action mailed on 02

November 2006 states, "Examiner asserts that saving instruction traces is common in

the art and can be utilized for many debugging purpose. Alverson/Angelo would have

been motivated to utilize this technique to gather more debugging/security information

for analysis." Page 12 of the Office Action similarly discusses motivation with regard to

claims 17 and 37.

Appellant has either overlooked or chosen not to address this motivation. For

that reason, it is presumed to be adequate.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or Board is identified by the examiner in the

Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejection should be sustained.
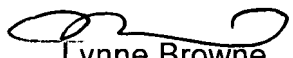
Respectfully submitted,

Brian P. Johnson

07 December 2006

Conferees:

Eddie Chan

Lynne Browne
APPEAL PRACTICE SPECIALIST, TQAS
TECHNOLOGY CENTER 2100

ALFORD KINDRED
PRIMARY EXAMINER